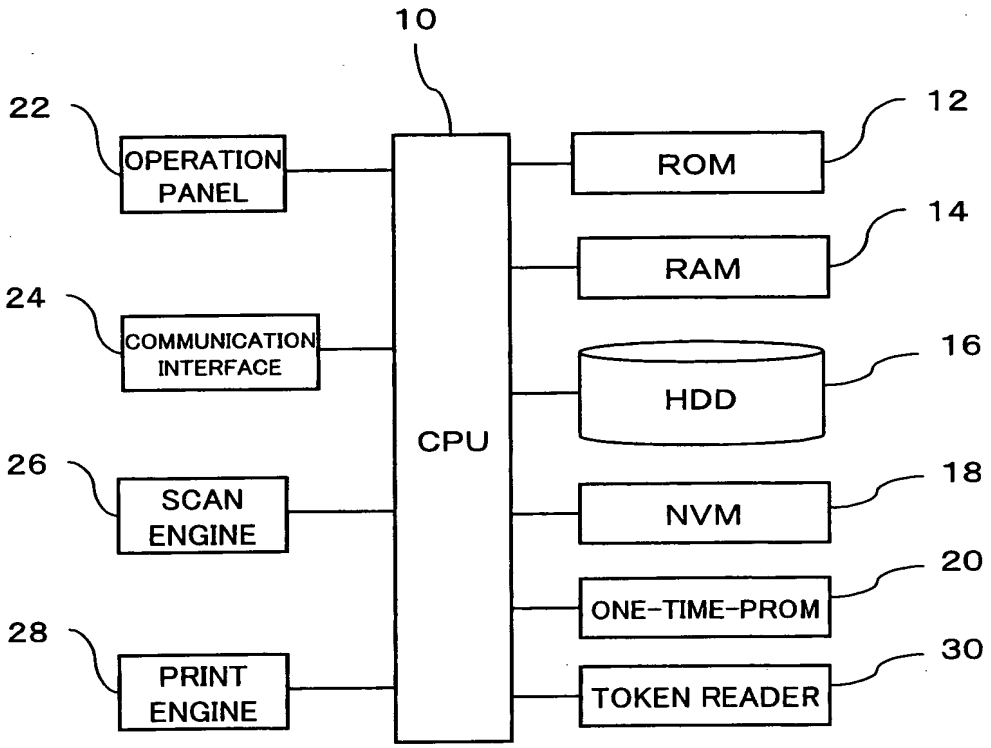
10
22
OPERATION PANEL
24
COMMUNICATION INTERFACE
26
SCAN ENGINE
28
PRINT ENGINE
CPU
12
ROM
14
RAM
16
HDD
18
NVM
20
ONE-TIME-PROM
30
TOKEN READER

FIG. 1

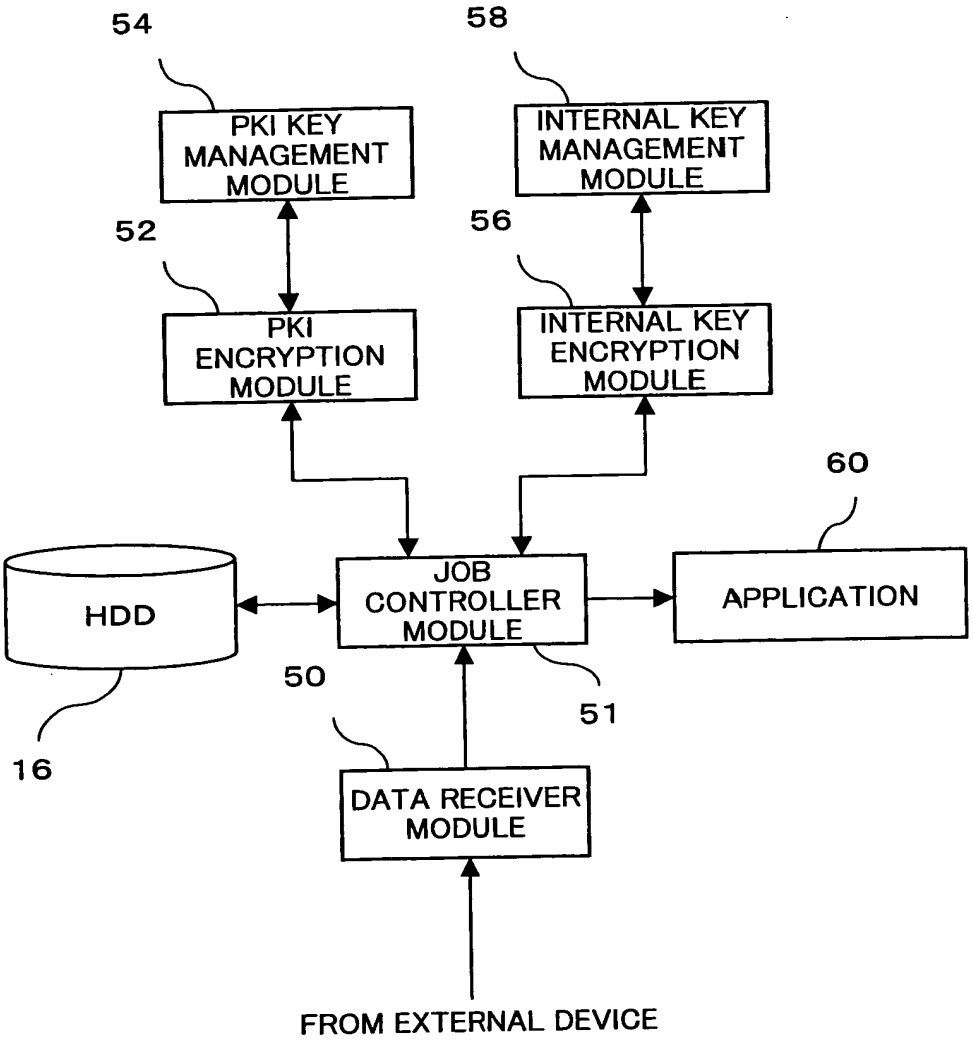
54
PKI KEY MANAGEMENT MODULE
52
PKI ENCRYPTION MODULE
58
INTERNAL KEY MANAGEMENT MODULE
56
INTERNAL KEY ENCRYPTION MODULE
60
HDD
JOB CONTROLLER MODULE
APPLICATION
50
51
16
DATA RECEIVER MODULE
FROM EXTERNAL DEVICE

FIG. 2

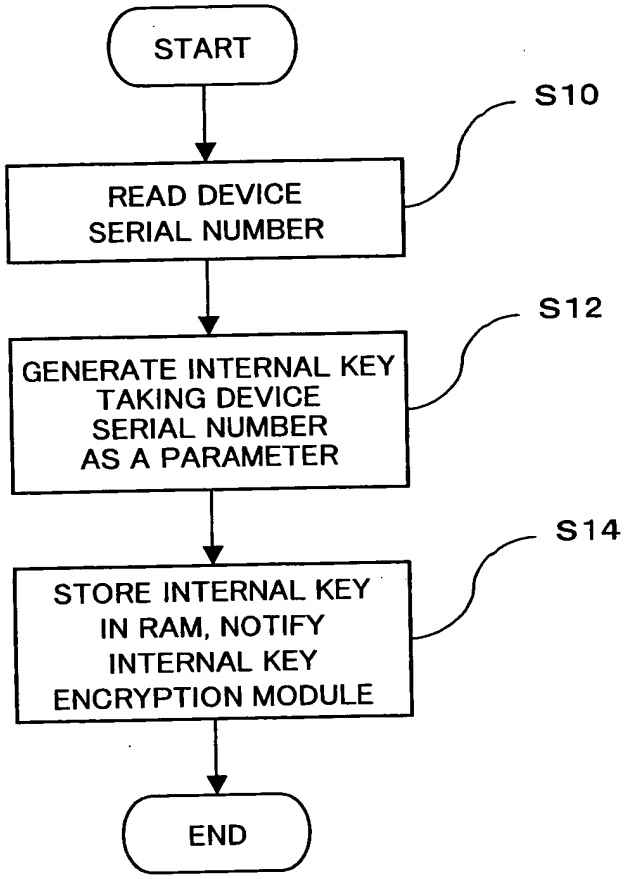
START
S10
READ DEVICE SERIAL NUMBER
S12
GENERATE INTERNAL KEY TAKING DEVICE SERIAL NUMBER AS A PARAMETER
S14
STORE INTERNAL KEY IN RAM, NOTIFY INTERNAL KEY ENCRYPTION MODULE
END

FIG. 3

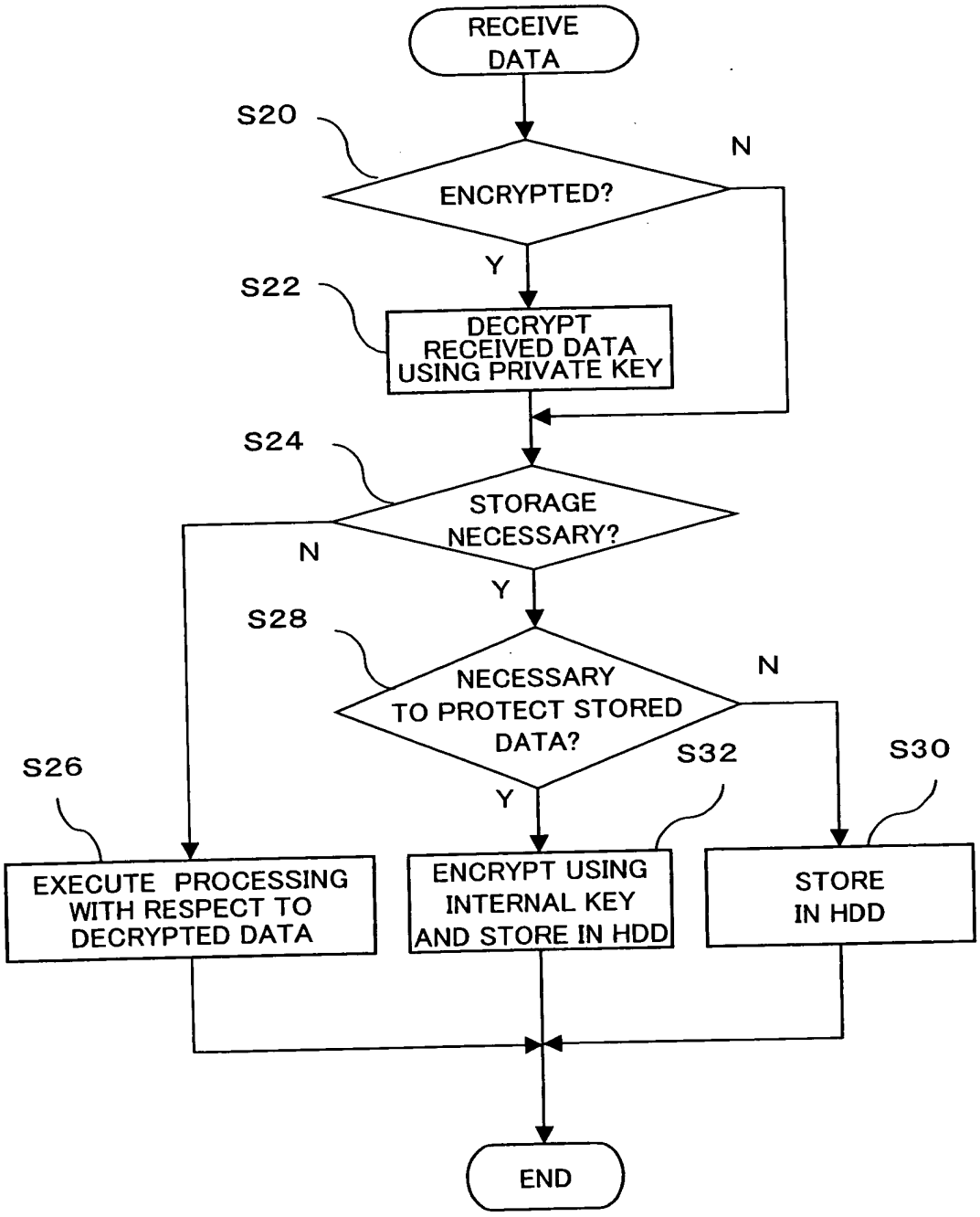
RECEIVE DATA
S20
ENCRYPTED?
N
Y
S22
DECRYPT RECEIVED DATA USING PRIVATE KEY
S24
STORAGE NECESSARY?
N
Y
S28
NECESSARY TO PROTECT STORED DATA?
N
Y
S26
S32
S30
EXECUTE PROCESSING WITH RESPECT TO DECRYPTED DATA
ENCRYPT USING INTERNAL KEY AND STORE IN HDD
STORE IN HDD
END

FIG. 4

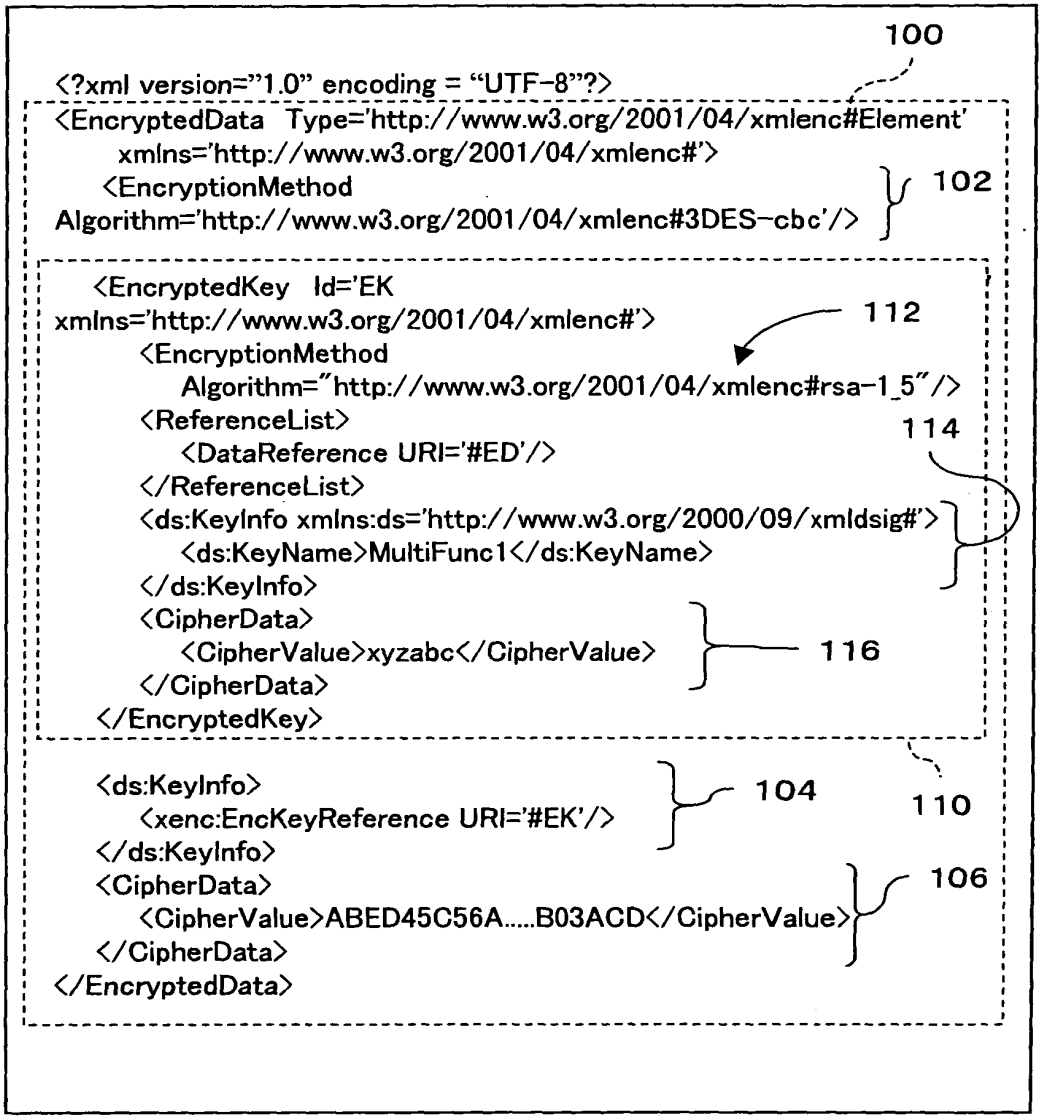
100
<?xml version="1.0" encoding = "UTF-8"?>
<EncryptedData Type='http://www.w3.org/2001/04/xmlenc#Element'
xmlns='http://www.w3.org/2001/04/xmlenc#'>
<EncryptionMethod
Algorithm='http://www.w3.org/2001/04/xmlenc#3DES-cbc'/>
102
<EncryptedKey Id='EK
xmlns='http://www.w3.org/2001/04/xmlenc#'>
112
<EncryptionMethod
Algorithm="http://www.w3.org/2001/04/xmlenc#rsa-1_5"/>
<ReferenceList>
114
<DataReference URI='#ED'/>
</ReferenceList>
<ds:KeyInfo xmlns:ds='http://www.w3.org/2000/09/xmldsig#'>
<ds:KeyName>MultiFunc1</ds:KeyName>
</ds:KeyInfo>
<CipherData>
<CipherValue>xyzabc</CipherValue>
116
</CipherData>
</EncryptedKey>
<ds:KeyInfo>
<xenc:EncKeyReference URI='#EK'/>
104
110
</ds:KeyInfo>
<CipherData>
<CipherValue>ABED45C56A.....B03ACD</CipherValue>
106
</CipherData>
</EncryptedData>

FIG. 5

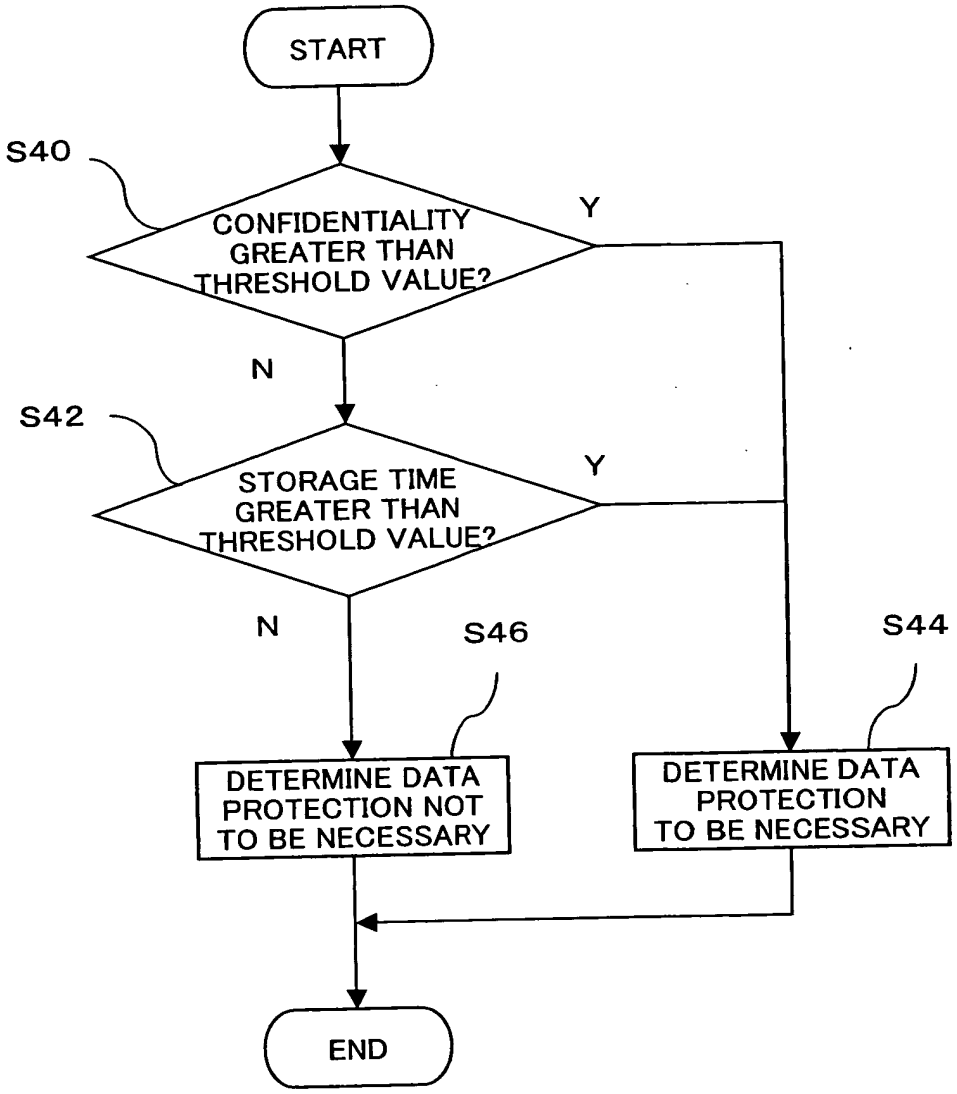
START
S40
CONFIDENTIALITY GREATER THAN THRESHOLD VALUE?
Y
N
S42
STORAGE TIME GREATER THAN THRESHOLD VALUE?
Y
N
S46
S44
DETERMINE DATA PROTECTION NOT TO BE NECESSARY
DETERMINE DATA PROTECTION TO BE NECESSARY
END

FIG. 6

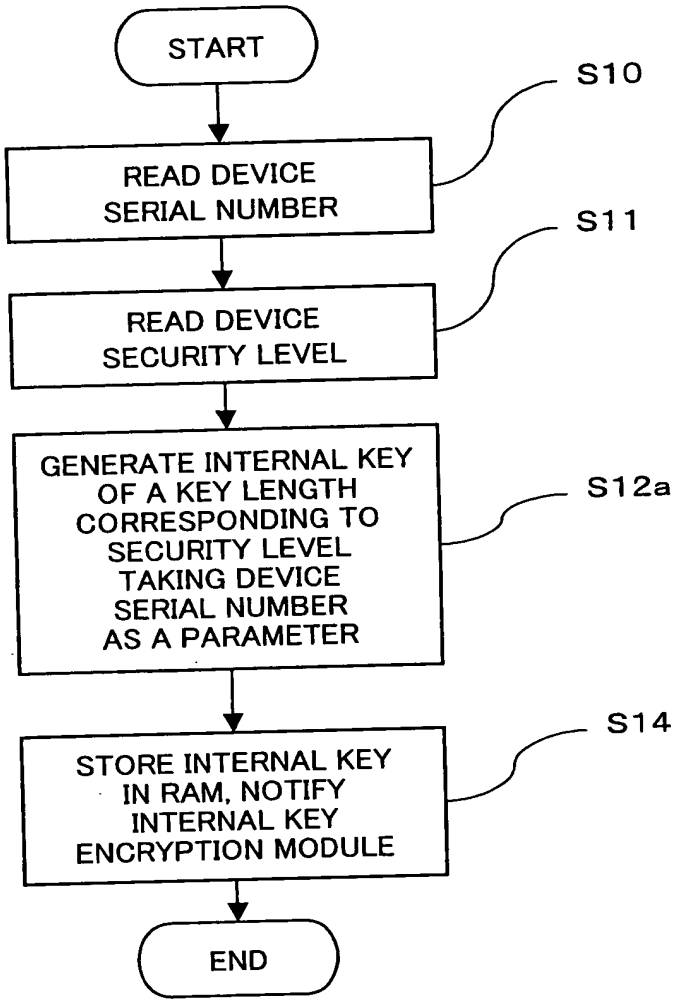
START
S10
READ DEVICE SERIAL NUMBER
S11
READ DEVICE SECURITY LEVEL
GENERATE INTERNAL KEY OF A KEY LENGTH CORRESPONDING TO SECURITY LEVEL TAKING DEVICE SERIAL NUMBER AS A PARAMETER
S12a
STORE INTERNAL KEY IN RAM, NOTIFY INTERNAL KEY ENCRYPTION MODULE
S14
END

FIG. 7

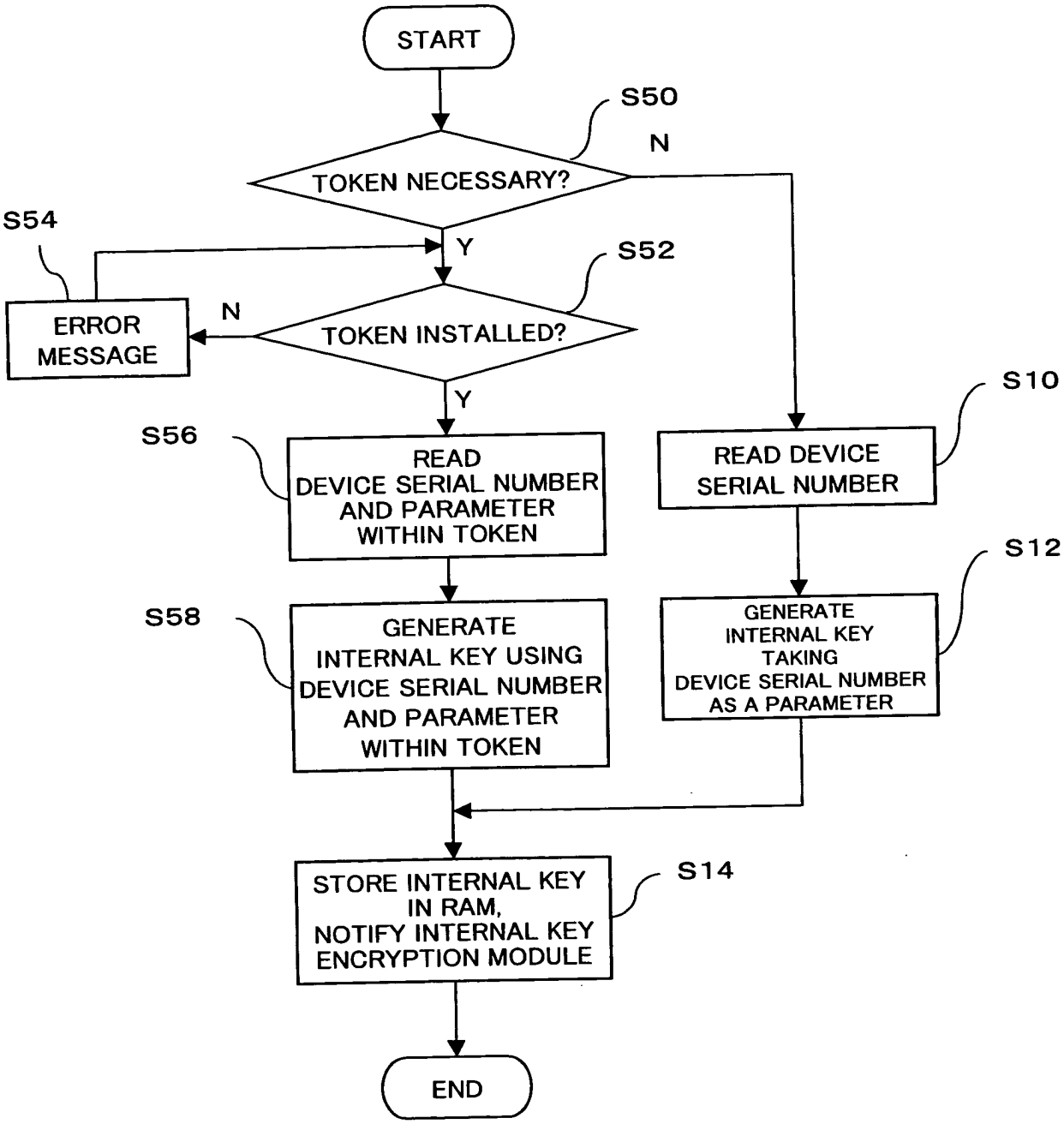
START
S50
TOKEN NECESSARY?
N
Y
S54
S52
ERROR MESSAGE
N
TOKEN INSTALLED?
Y
S10
S56
READ DEVICE SERIAL NUMBER
READ DEVICE SERIAL NUMBER AND PARAMETER WITHIN TOKEN
S12
S58
GENERATE INTERNAL KEY TAKING DEVICE SERIAL NUMBER AS A PARAMETER
GENERATE INTERNAL KEY USING DEVICE SERIAL NUMBER AND PARAMETER WITHIN TOKEN
S14
STORE INTERNAL KEY IN RAM, NOTIFY INTERNAL KEY ENCRYPTION MODULE
END

FIG. 8